| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/544,898 | 04/07/2000 | George H. Peden | 004698.P002 | 2445 |

7590    03/28/2003

FINNEGAN, HENDERSON, FARABOW
GARRETT & DUNNER L L P
1300 I STREET N W
WASHINGTON, DC   20005-3315

| EXAMINER |
|---|
| ALAM, UZMA |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2157 | |

DATE MAILED: 03/28/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 07-01)

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

   A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
   THE MAILING DATE OF THIS COMMUNICATION.
   - Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
      after SIX (6) MONTHS from the mailing date of this communication.
   - If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
   - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
   - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
   - Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
      earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒   Responsive to communication(s) filed on _07 April 2000_ .

2a)☐   This action is **FINAL**.          2b)☒   This action is non-final.

3)☐   Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
       closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒   Claim(s) _1-30_ is/are pending in the application.

       4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐   Claim(s) _____ is/are allowed.

6)☒   Claim(s) _1-30_ is/are rejected.

7)☐   Claim(s) _____ is/are objected to.

8)☐   Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☒   The specification is objected to by the Examiner.

10)☒   The drawing(s) filed on _07 April 2000_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

       Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐   The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

       If approved, corrected drawings are required in reply to this Office action.

12)☐   The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

13)☐   Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

       a)☐ All   b)☐ Some *   c)☐ None of:

           1.☐   Certified copies of the priority documents have been received.

           2.☐   Certified copies of the priority documents have been received in Application No. _____ .

           3.☐   Copies of the certified copies of the priority documents have been received in this National Stage
                 application from the International Bureau (PCT Rule 17.2(a)).
       * See the attached detailed Office action for a list of the certified copies not received.

14)☐   Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

       a) ☐ The translation of the foreign language provisional application has been received.

15)☐   Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

| | |
|---|---|
| 1) ☒ Notice of References Cited (PTO-892) | 4) ☐ Interview Summary (PTO-413) Paper No(s). _____ . |
| 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) ☐ Notice of Informal Patent Application (PTO-152) |
| 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ . | 6) ☐ Other: . |

## DETAILED ACTION

### *Specification*

The disclosure is objected to because of the following informalities: on page 1, lines 5

and lines 7, there is no application number given.  Appropriate correction is required.

### *Claim Rejections - 35 USC § 112*

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 28 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for

failing to particularly point out and distinctly claim the subject matter which applicant regards as

the invention.

Claim 28 recites the limitation "machine readable storage medium" in claim 7.  There is

insufficient antecedent basis for this limitation in the claim.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999

(AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002

do not apply when the reference is a U.S. patent resulting directly or indirectly from an

international application filed before November 29, 2000. Therefore, the prior art date of the

reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA

35 U.S.C. 102(e)).

Claims 1-5, 7, 9, 11, 13, 14, 19, 20, 22, 24, 26, 27, 29, and 30 are rejected under 35

U.S.C. 102(e) as being anticipated by Russell US Patent No. 5,455,953. See abstract.


As per claim 1, Russell discloses a method comprising:

receiving a request for a ticket at a ticket server, said request being from a client, said

ticket to qualify the client to access a key from a key server, said key to facilitate an event

between the client and at least one additional client (column 3, lines 35-50; column 5, lines 4-26;

column 10, lines 1-20);

determining if the client is authorized to receive the key (column 3, lines 51-63); and

transmitting the ticket from the ticket server to the client if the client is authorized

(column 3, lines 41-50).

As per claim 2, Russell discloses the method of claim 1 wherein determining if the client

is authorized comprises:

accessing a database that defines authorized clients (column 10, lines 21-24; column 12

lines 64-67; column 22, lines 1-11)); and

determining if the client is among the authorized clients defined by the database (column

10, lines 24-33; column 11, lines 1-10; column 22, lines 51-58).


As per claim 3, Russell discloses the method of claim 1 further comprising:

accessing a database that defines associations between authorized clients and events

(column 22, lines 2-11);

constructing a summary of all events to which the client is associated based on the

database (column 22, lines 12-31); and

including the summary in the ticket (column 22, lines 12-31 and 51-58; column 23, lines

20-29).


As per claim 4, Russell discloses the method of claim 3 wherein the database comprises a

directed hierarchy of groups, wherein each group comprises at least one member client and/or at

least one member event, and wherein constructing the summary comprises:

locating a particular group in the database to which the client is a member client (column

18, lines 20-46);

adding identifying information to the summary for each event, if any, belonging to the

particular group (column 19, lines 60-67; column 20, lines 1-3);

locating at least one ancestor group to the particular group in the directed hierarchy of groups

(column 22, lines 2-31); and

adding identifying information to the summary for each event, if any, belonging to the at

least one ancestor group (column 22, lines 59-66).

As per claim 5, Russell discloses the method of claim 1 wherein the ticket comprises at

least one of an identifier that indicates a group to which the client belongs, a list identifying at

least one event for which the client is qualified, and a digital certificate that indicates that the

client is authorized for each listed event (column 23, lines 46-60; column 24, lines 1-20).

As per claim 7, Russell discloses a method comprising:

receiving a request for a key at a key server, said request being received from a client,

and said key to facilitate an event between the client and at least one additional client (column 3,

lines 35-50; column 5, lines 4-26; column 10, lines 1-20);

determining if the client is qualified to receive the key based on a ticket previously

obtained by the client from a ticket server (column 3, lines 5-63; column 24, lines 44-67); and

transmitting the key from the key server to the client if the client is qualified (column 3,

line 41-50; column 24, lines 44-67).

As per claim 9, Russell discloses the method of claim 7 wherein the client is one of a

receiving client and a sending client (column 23, lines 30-45).

As per claim 11, Russell discloses the method of claim 7 further comprising:

establishing a secure point-to-point link between the key server and the client in response

to the requests, wherein the key is transmitted over the secure point-to-point link (column 8, lines

44-65).

As per claim 13, Russell discloses the method of claim 7 wherein the key corresponds to

a first interval of the event, and wherein the method further comprises:

determining if the client remains qualified to receive a refresh key (column 10, lines 21-

33; column 23, lines 1-19; column 24, lines 44-67); and

transmitting the refresh key to the client if the client remains qualified, said refresh key

corresponding to a subsequent interval of the event (column 10, lines 21-53).

As per claims 14 and 27, Russell discloses the method of claim 7 and the machine

readable storage medium of claim 22 wherein the key corresponds to a first interval of the event,

and wherein the method further comprises:

receiving a plurality of additional requests for the key from a plurality of additional clients

(column 10, lines 1-33);

determining if the each of the plurality of additional clients are qualified to receive the

key based on a ticket previously obtained by each of the plurality of additional clients from the

ticket server (column 3, lines 5-63; column 24, lines 44-67);

transmitting the key to each of the plurality of additional clients that are qualified (column 3,

lines 41-50; column 24, lines 44-67);

determining if the client and each of the plurality of additional clients remain qualified to

receive a refresh key (column 10, lines 21-33; column 23, lines 1-19; column 24, lines 44-67);

and    transmitting the refresh key to the client if the client remains qualified and to each of the

plurality of additional clients that remain qualified, said refresh key corresponding to a

subsequent interval of the event (column 10, lines 21-53).


As per claim 19, Russell discloses a machine readable storage medium having stored

thereon machine executable instructions, execution of said machine executable instructions to

implement a method comprising:

obtaining a ticket at a client from a ticket server, said ticket defining an event between the

client and at least one additional client (column 3, lines 35-50; column 10, lines 1-20; column 5,

lines 4-26);

obtaining a key at the client from a key server based on the ticket (column 22, lines 2-31);

and participating in the event with the at least one additional client based on the key

(column 3, lines 41-63).


As per claim 20, Russell discloses the machine readable storage medium of claim 19

wherein obtaining the ticket comprises:

sending a request to the ticket server for a list of events in which the client is qualified to

participate (column 3, lines 41-50; column 22, lines 2-31).

As per claim 22, Russell discloses a machine readable storage medium having stored thereon machine executable instructions, the execution of said machine executable instructions to implement a method comprising:

receiving a request for a key at a key server, said request being received from a client, and said key to facilitate an event between the client and at least one additional client (column 3, lines 35-50; column 10, lines 1-20; column 5, lines 4-26);

determining if the client is qualified to receive the key based on a ticket previously obtained by the client from a ticket server 9column 3, lines 51-63; column 5, lines 4-26; column 10, lines 1-20; column 24, lines 44-67); and

transmitting the key from the key server to the client if the client is qualified (column 3, lines 41-50; column 24, lines 44-67).

As per claim 24, Russell discloses the machine readable storage medium of claim 22 further comprising:

establishing a secure point-to-point link between the key server and the client in response to the request, wherein the key is transmitted over the secure point-to-point link (column 8, lines 44-65).

As per claim 26, Russell discloses the machine readable storage medium of claim 22 wherein the key corresponds to a first interval of the event, and wherein the method further comprises:

determining if the client remains qualified to receive a refresh key (column 10, lines 21-33; column 23, lines 1-19); and

transmitting the refresh key to the client if the client remains qualified, said refresh key corresponding to a subsequent interval of the event (column 10, lines 21-53).

As per claim 29, Russell discloses a ticket server apparatus comprising:

a port to receive a request for a ticket, said request being from a client, said ticket to qualify the client to access a key from a key server, said key to facilitate an event between the client and at least one additional client (column 3, lines 35-50; column 5, lines 4-26; column 10, lines 1-20); and

circuitry to determine if the client is authorized to receive the key, and to transmit the ticket through the port to the client if the client is authorized (column 3, lines 41-63).

As per claim 30, Russell discloses a key server apparatus comprising: a port to receive a request for a key, said request being received from a client, and said key to facilitate an event between the client and at least one additional client (column 3, lines 35-50; column 5, lines 4-26; column 10, lines 1-20); and

circuitry to determine if the client is qualified to receive the key based on a ticket previously obtained by the client from a ticket server, and to transmit the key through the port to the client if the client is qualified (column 3, lines 41-50; column 24, lines 44-67).

## *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Russell US Patent

No. 5,455,953 in view of Massarani US Patent No. 6,393,484.

As per claim 6, Russell discloses the method of claim 5 wherein the list comprises at least

one of certain fields (column 23, lines 46-60; column 24, lines 1-20). Russell does not expressly

disclose fields which contain a title of each listed event, an internet protocol (IP) address for each

listed event, a time indication for each listed event, and an IP address for a key server

corresponding to each listed event. Massarani discloses a database which stores a list of IP

addresses and other user identification and associated parameters such as what events the user is

allowed to connect to (abstract; column 5, lines 26-54; column 6, lines 1-10; column 7, lines 10-

34). At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to combine the fields of Russell with the specific entries for each field of the

Massarani. A person of ordinary skill in the art would have been motivated to do this because

the specifics given in the claim are just descriptions of the user which are part of a user profile

which Russell describes with his fields and it would ensure the more accurate authentication of a user.

Claims 8, 10, 12, 16-18, 21, 23, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Russell US Patent No. 5,455,953 in view of Wollrath et al. US Patent No. 6,519,615.

As per claim 8, Russell discloses the method of claim 7 wherein the key comprises at least one of a symmetric cryptographic key (column 22, lines 21-39; column 23, lines 20-29). Russell does not expressly disclose "keys for the event, an initiation time for use of the key, and a lifetime for the key. Wollrath discloses an initiation time for the use of the key and a lifetime for the key (abstract; column 8, lines 8-22 and lines 62-67; column 12, lines 34-47) At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to combine the keys of Russell with the specifications of the duration of the keys of Wollrath. A person of ordinary skill in the art would have been motivated to do this to add the advantage of extra security when authorizing a user.

As per claims 10 and 23, Russell discloses "the method of claim 7 and the machine readable storage medium of claim 22 wherein the request comprises an initial request for the event (See claim 7 and claim 22 above and column 7, lines 1-9)." Russell does not expressly disclose "wherein receiving the initial request comprises receiving the initial request at a

particular time during a predetermined period before the event, said particular time being

randomly generated by the client". Wollrath discloses requesting at a predetermined time before

the event. See column 8, lines 8-22; column 9, lines 1-8. At the time the invention was made, it

would have been obvious to a person of ordinary skill in the art to combine the initial request of

Russell with the time frame of the request of Wollrath. A person of ordinary skill in the art

would have been motivated to do this to give secure access to a user before the event that the

user needs it or based on a certain time frame to reduce the possibility of unauthorized access.

As per claims 12 and 25, Russell discloses the method of claim 7 and the machine

readable storage medium of claim 22 (see claims 7 and 22 above). Russell does not expressly

disclose "Wherein the request comprises one of a plurality of refresh requests, wherein each of

the plurality of refresh requests corresponds to one of a plurality of forward security windows

during the event, wherein each of the plurality of forward security windows comprises a repeated

time interval, and wherein receiving the refresh request comprises:

receiving the refresh request at a particular time within a corresponding forward security

window, said particular time being randomly generated by the client for a first forward security

window and applied at the repeated time interval thereafter". Wollrath discloses receiving the

request at a particular time. See abstract, column 8, lines 8-22 and 62-67; column 9, lines 1-10.

See claim 10 above.

As per claim 16, Russell discloses the method of claim 7 wherein the key server has a

synchronized time with respect to a sending client for the event to within a margin of error, and

wherein the method further comprises:

determining which of a plurality of available keys to use for said key (column 21, lines 64-67; column 22, lines 1-39). Russell does not disclose "based on the synchronized time." Wollrath discloses giving access at a certain time. See (column 4, lines 43-67; column 8, lines 8-22 and 62-67; column 9, lines 1-7). See claim 10 above.

As per claim 17, Russell discloses the method of claim 7 wherein determining comprises at least one of:

verifying that the request includes credentials for the event (column 3, lines 9-25 and 36-63). Russell does not expressly disclose "verifying that the request is received within a predetermined period before the event or time interval during the event." Wollrath discloses giving access base on time. See column 4, lines 43-67; column 8, lines 8-22 and 62-67; column 9, lines 1-7. See claim 10 above.

As per claim 18, Russell discloses the method and the machine readable storage medium of claim 7 (see claim 7 above). Russell does not disclose "wherein the request is received within a predetermined time frame after the event starts, wherein said event is not encrypted during the predetermined period." Wollrath discloses receiving a request within a certain time frame. See column 13, lines 21-56. See claim 10 above.

As per claim 21, Russell discloses the machine readable storage medium of claim 19 wherein obtaining the key comprises:

receiving an indication to participate in the event (column 7, lines 1-9). Russell does not

disclose "initiating a transaction with the key server at a location indicated by the ticket and

within a time frame prior to a start time of the event indicated by the ticket." Wollrath discloses

initiating a transaction bases on a certain time frame. See column 8, lines 8-22; column 9, lines

1-8. See claim 10 above.


Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Russell US

Patent No. 5,455,953 in view of Yuasa et al. US Patent No 6,085,238.


As per claim 15, Russell discloses the method of claim 14 further comprising:

establishing a secure multicast link from the key server to the client and the plurality of

additional clients, wherein the refresh key is transmitted through the network (column 1, lines

26-35; column 3, lines 9-25). Russell does not expressly disclose "a secure multicast link."

Yuasa discloses a secure multicast link (column 21, lines 34-51) At the time the invention was

made, it would have been obvious to a person of ordinary skill in the art to combine the network

of Russell with the multicast link of Yuasa. A person of ordinary skill in the art would have been

motivated to do this because the secure multicast links allow for high-speed communication so it

would reduce the time that it took to authenticate a user.

## *Conclusion*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Veluvali U.S. Patent No. 6,477,559 discloses secure access to a system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Uzma Alam whose telephone number is (703) 305-8420. The examiner can normally be reached on Monday - Friday 8:30 - 5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on (703) 308 - 7562. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 308-9052 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9600.

ua
March 24, 2003

ARIO ETIENNE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100